ICO consultation on the draft right of access guidance

The right of access (known as subject access) is a fundamental right of the General Data Protection Regulation (GDPR). It allows individuals to find out what personal data is held about them and to obtain a copy of that data. Following on from our initial GDPR guidance on this right (published in April 2018), the ICO has now drafted more detailed guidance which explains in greater detail the rights that individuals have to access their personal data and the obligations on controllers. The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the exemptions that are most likely to apply in practice when handling a request.

We are running a consultation on the draft guidance to gather the views of stakeholders and the public. These views will inform the published version of the guidance by helping us to understand the areas where organisations are seeking further clarity, in particular taking into account their experiences in dealing with subject access requests since May 2018.

If you would like further information about the consultation, please email SARguidance@ico.org.uk.

Please send us your response by 17:00 on **Wednesday 12 February 2020**.

Privacy statement

For this consultation, we will publish all responses received from organisations but we will remove any personal data before publication. We will not publish responses received from respondents who have indicated that they are an individual acting in a private capacity (e.g. a member of the public). For more information about what we do with personal data see our privacy notice.

Please note, your responses to this survey will be used to help us with our work on the right of access only. The information will not be used to consider any regulatory action, and you may respond anonymously should you wish.

Please note that we are using the platform Snap Surveys to gather this information. Any data collected by Snap Surveys for ICO is stored on UK servers. You can read their Privacy Policy.

Q1 Does the draft guidance cover the relevant issues about the right of access?

- ☒ Yes
- ☐ No
- ☐ Unsure/don't know

If no or unsure/don't know, what other issues would you like to be covered in it?

Yes, subject to some suggested additions below.

Q2 Does the draft guidance contain the right level of detail?

- ☒ Yes
- ☐ No
- ☐ Unsure/don't know

If no or unsure/don't know, in what areas should there be more detail within the draft guidance?

Yes, though there are some areas where additional points could helpfully be covered. See comments below.

Q3 Does the draft guidance contain enough examples?

- ☐ Yes
- ☒ No
- ☐ Unsure/don't know

If no or unsure/don't know, please provide any examples that you think should be included in the draft guidance

On page 5, it would be more instructive to have **an example where the Processor would have data the Controller would not possess itself**.

- One option could be a global company that uses a third-party relocation company to help them move staff around the world. That relocation company would collect info the employer wouldn't have itself.
- Another option could be a provider of background checks that acts as a processor for employers.

An example on page 12 of a third party lodging a SAR would be helpful. This **could helpfully relate to new 'platforms'** that seek to use DSARs to help individuals better control their personal data. Examples include:
- Tapmydata - https://tapmydata.com/
- WeAreDavid - https://weredavid.com/?page=about.html

An example on page 24 of **what does / does not constitute a SAR** would be helpful.

Q4 We have found that data protection professionals often struggle with applying and defining 'manifestly unfounded or excessive' subject access requests. We would like to include a wide range of examples from a variety of sectors to help you. Please provide some examples of manifestly unfounded and excessive requests below (if applicable).

We have provided comments on this issue in a separate letter, already submitted to the ICO.

As a further point, **we recommend making it more explicit** on page 22 that where the controller is not satisfied that the third party has appropriate authorization or is acting fraudulently, the controller does not need to comply with the SAR.

We would also reiterate that, consistent with prior ICO advice, the guidance should **make clear on pages 21-22 that firms can set up 'short form' processes for bulk SARs** and that the controller can agree with the third party for such a process to be used.

Lastly, we agree that this is a challenging area. We suggest that the ICO **publish suitably anonymized examples of good / bad practice as these emerge**.

Q5 On a scale of 1-5 how useful is the draft guidance?

1 – Not at all useful	2 – Slightly useful	3 – Moderately useful	4 – Very useful	5 – Extremely useful
☐	☐	☒	☐	☐

Q6 Why have you given this score?

In many respects the guidance is very helpful. However, as per our comments in this paper, there are areas where we think changes are needed to make the final document more pragmatic and ensure that the personal data and other interests of individuals are effectively protected. In addition to our comments here, we outline our concerns on this specific issue in our separate letter sent to the ICO in January.

Q7 To what extent do you agree that the draft guidance is clear and easy to understand?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
☐	☐	☐	☒	☐

Q8 Please provide any further comments or suggestions you may have about the draft guidance.

We presume that the ICO intends to retain its guidance on access to information in complaint files, which is also helpful, particularly in relation to:

- distinguishing what data relates to the requestor, third parties or both
- opinions that might contain personal data
- search of email regarding whether the content is commercially focused or 'relates to' the individual

We **recommend sign posting this other guidance in the SARs guidance**, given it will often be relevant: https://ico.org.uk/media/for-organisations/documents/1179/access_to_information_held_in_complaint_files.pdf

Page 11 – The second-to-last paragraph suggests that, where a controller receives a SAR from a third party, the controller should ask the data subject whether it would be acceptable to send the SAR response to him/her directly, rather than to the third party. The GDPR does not require this so **firms should be able to share the response directly with the data subject rather than having to get customer consent**, when it is more appropriate to do so (consistent with previous guidance on this topic from the ICO, notably a bulletin to claims management companies in September 2018). This is particularly important where the controller has concerns about information security or wider data protection standards at the third party. This is especially relevant where the third party making the request is claims management company or other bulk submitter.

Guidance on page 13 suggests that in England, Wales and Northern Ireland, when a controller receives a SAR from an individual aged between 13 and 16, the controller must assess the child's maturity and ability to understand the right being invoked. The guidance should **make clear that the controller can make a standard internal policy,** rather than having to make a case-by-case assessment. Financial services firms are unlikely to have an easy means to assess the maturity of the individual.

Pages 16-17 and 24: It is important to clarify here that where a controller is already processing a SAR but **the individual then expands the scope of the data request, the controller can consider this to be a fresh SAR**, with a fresh 30 day period to provide the new information. This can arise for example when the individual had advised that he/she was interested in specific information, but then later contacts the controller to say that additional information is also sought, eg: to cover a wider time period, add additional controllers, expand data types, etc. Similarly, this can arise if a controller is doing a full, generic 'reasonable search' but then some time later the data subject clarifies the SAR and makes clear that he/she is interested in data that would not be caught by a standard 'reasonable search'. This is an important detail to clarify, as the current guidance suggests that firms might have to, in effect, complete a full search in an impossibly short time (eg: do in effect a full SAR process in 24 hours if the individual expands the scope 29 days after making the initial request).

The page 18 discussion of 'complex requests' should be expanded, as this is a challenging area. **We recommend making clear that the following are also factors that increase complexity**:

- needing to search **unstructured data,** such as the content of emails neither to nor from the data subject
- needing to review emails or other items to determine whether they contain **third party information**
- needing to review emails or other items to determine **whether they contain personal data** (this can be complex, for example where other information would be needed in order to identify the individual)

Pages 19-21 –

- There may be situations where the controller does not have / has not had any relationship with the requester and does not know the individual. When confirming the individual's identity, the company may then be processing personal data about an individual previously unknown to them.
- Confirming back to the requestor that there is no personal data held about the individual *could be used against that individual* if the request was in fact made by some third party (where the two parties are involved in litigation, for instance). **Does ICO have any recommendations on how to approach such requests** coming from individuals that are not known to the controller, aside from verifying the identity and authorization from the data subject?

Page 20 –

- The guidance implies that controllers cannot reasonably ask for ID when the individual is known, with an employee known personally to another employee given as an example. This risks leaving a lot up to the discretion and subjective view of individual employees, and creates some risk of mis-use or mis-application by employees, putting the controller at risk of breaching confidentiality obligations. **Firms should be able to have proportionate policies about identity verification that are not left to individual employee discretion**, especially in the financial services sector, as there is a significant risk of fraud if SAR responses are sent to the wrong person.
- Further to this point: the example might be a suitable analysis in the context of a small business but for firms that have 10,000s of employees, it is not the case that the firm will necessarily 'know the individual personally'. Full ID / verification might be needed, particularly as firms will not necessarily have a personal email address available to use in verification. Given the stricter standard applied in the second example on page 20 in relation to a customer, the implication is that firms should make less effort to confirm the identity of individuals claiming to be employees. This means, in effect, a lower degree of protection for employees.
- Also, where the controller does not have an ongoing relationship with the individual, confirming ID can be more challenging and more care is often needed. It would be **helpful for the guidance to acknowledge this**. This point is also relevant in relation to pages 10-12 (SARs lodged by third parties).

Pages 23-24:

- The guidance refers to a 'reasonable search' where a data subject does not provide clarifying information to help locate the relevant personal data. Setting the standard at 'reasonable' is a welcome clarification.
- However, in our view it is not proportionate to expect controllers to immediately start a full search for personal data (even if this is limited to a 'reasonable search') in some situations. In particular:
    - In some contexts, such as in relation to an employee SAR where the scope is not limited to a certain time period, type of data, etc, a search can give hundreds of millions of results. When very large amounts of data relating to an individual are held, controllers should have a reasonable opportunity to liaise with the individual and clarify the scope of the data of interest before 'starting the clock'. This is particularly important when it is unclear where the relevant data might be stored, or when the data held is particularly diverse.
    - When it is clear that the individual is looking for specific data but has not provided sufficient information for the controller to be able to determine what that information is. This can arise when customers / ex-customers ask about very old / closed bank accounts, for example. Some of our members receive such queries in their hundreds.
- Not giving sufficient opportunity to controllers to clarify the scope of data sought risks pushing towards a situation where data subjects are frequently overwhelmed with data of little interest to them, which would not be in their interests. The current guidance would also mean that firms will sometimes need to start a resource-intensive search, only to then discard much of the data once the request has been clarified, wasting resources and staff time that could be more helpfully employed responding promptly to well-defined DSARs. **We recommend returning to the position under the former SAR code of practice**, which stated on page 28:
    - "Before responding to a SAR, you may ask the requester for information you reasonably need to find the personal data covered by the request. You need not comply with the SAR until you have received it. However, even if the relevant information is difficult to find and retrieve, it is not acceptable for you to delay responding to a SAR unless you reasonably require more information to help you find the data in question." [Emphasis added].
- We also suggest revising the wording of the first sentence of the last paragraph on page 23: "You cannot ask the requester to narrow the scope of their request." This seems to suggest that, if a SAR is received with no indication of what specific information is sought, the controller must provide all data held and cannot engage with the individual to identify the specific data of interest. We do not think that this is what the ICO intends; indeed, the example on page 24 seems to clearly describe an 'unbounded' SAR coming in from an employee, the controller then suggesting that the SAR's scope be narrowed, and the employee then clarifying his/her interest. Provided controllers do not unduly pressure individuals to narrow the scope of a SAR, this kind of engagement and constructive discussion seems beneficial for all parties. **We recommend revising the wording of the last paragraph of page 23 to make clear that good faith suggestions to clarify what information is of interest are legitimate.** This would better align with the example on page 24 and with the second-to-last paragraph on page 23.

The example on page 24 is confusing. The existence of third-party personal data would trigger other GDPR and DPA considerations (eg: GDPR Article 15(4)). Given what the example is intended to illuminate, it would be clearer to **just focus on the existence of customer and employee data about the individual**.

Comments in relation to page 29:

- It would be helpful to reiterate the point on page 15 that **some documents**, particularly correspondence already provided to the data subject, **would often not need to be treated as in scope of a SAR**.
- It would be helpful to also clarify here that where the data subject already has access to the information, the **controller can reasonably explain to him/her how to access the information**, rather than having to provide it. For example, where an employee already has access to information through his/her inbox, etc.

Page 30: The guidance states that if the SAR is lodged electronically, the firm must send the data in electronic format. This makes sense as a default, but **the guidance should recognize that the individual can ask for a response in hard copy**. At present, the guidance suggests that the controller should refuse such a request and provide the information electronically despite the individual's wishes.

Page 31: We recognize that technology changes and that the ICO will not want to provide an exhaustive list, but **some indicative examples of appropriate format** would be helpful in relation to requests for audio/visual data. Suitable examples would include, in our view, DVD, CDROM and on USB. Some examples of suitable file types would also be helpful.

Pages 47, 55, and 57 contain helpful examples relating to exemptions from the normal right of access rules. It would be useful to **note that these exemptions could be time bound**, eventually ceasing to apply if in due course there is another SAR and the investigation / business change / negotiation is no longer at risk of being undermined by supplying the personal data.

On page 61 it could be helpful to **mention some other types of data potentially held by CRAs** so that it is clear that more data exists than just individuals' financial standing.

Q9 Are you answering as:

- ☐ An individual acting in a private capacity (eg someone providing their views as a member of the public)
- ☐ An individual acting in a professional capacity
- ☒ On behalf of an organisation
- ☐ Other

Please specify the name of your organisation:

UK Finance

What sector are you from:

UKF is a financial services trade association

Q10 How did you find out about this survey?

- ☐ ICO Twitter account
- ☐ ICO Facebook account
- ☐ ICO LinkedIn account
- ☒ ICO website
- ☒ ICO newsletter
- ☐ ICO staff member
- ☐ Colleague
- ☐ Personal/work Twitter account
- ☐ Personal/work Facebook account
- ☐ Personal/work LinkedIn account
- ☐ Other

Thank you for taking the time to complete the survey.